09673106
5050
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 464-I51177WO	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR99/00837	International filing date (*day/month/year*) 09 April 1999 (09.04.99)	Priority date (*day/month/year*) 09 April 1998 (09.04.98)
International Patent Classification (IPC) or national classification and IPC G07F 7/10		
Applicant INNOVATRON ELECTRONIQUE, SOCIETE ANONYME		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
04 November 1999 (04.11.99)	17 May 2000 (17.05.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR99/00837

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-15, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. 1-13, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. _____, filed with the letter of _____,
Nos. _____, filed with the letter of _____.

☐ the drawings, sheets/fig _____, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-13	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-13	NO
Industrial applicability (IA)	Claims	1-13	YES
	Claims		NO

2. Citations and explanations

The subject matter of claim 1 differs from the prior art known from document D1 (WO-A-89/02140) only in that a **plurality** of alteration instructions are applied to the card by the terminal.

Document D1, which is cited on page 1, lines 27-30 of the description of the present application, describes the application of only one alteration instruction at a time. Specifically, the aim of D1 is to prevent the card from being decremented unless the service paid for (telephone calls) is actually provided.

The method known from D1 comprises altering only one data item on the card. Therefore, the subject matter of claim 1 is novel.

Nevertheless, a person skilled in the art aware of the method described in D1 and seeking to apply said method to a teleticketing system, while guaranteeing to users that payment will not be made unless the service is provided (i.e. the ticket is debited from the card), would automatically and non-inventively increase the number of alteration instructions to be applied to the card by the terminal since, by definition, in teleticketing, the card has to be altered at least twice, namely for credit deduction and ticket issuing.

Therefore, a person skilled in the art would automatically arrive at the subject matter of claim 1 simply by adapting the teaching of document D1 to a use in teleticketing.

It follows that claim 1 fails to comply with the provisions of PCT Article 33 as its subject matter does not involve an inventive step.

The Examiner is of the opinion that the subject matter of all of dependent claims 2 to 13 can be derived in an obvious manner from the use of the method known from D1 in a teleticketing system. For example, in a teleticketing application, the generation of a certificate or authentication is necessary and thus obvious (see claims 5-10).

17
T

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 464-I51177WO	**POUR SUITE A DONNER**	voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)
Demande internationale n° PCT/FR99/00837	Date du dépot international *(jour/mois/année)* 09/04/1999	Date de priorité *(jour/mois/année)* 09/04/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G07F7/10		
Déposant INNOVATRON ELECTRONIQUE (SOCIETE ANONYME) et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 4 feuilles, y compris la présente feuille de couverture.

   ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☐ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 04/11/1999	Date d'achèvement du présent rapport 17.05.00
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Closa, D N° de téléphone +49 89 2399 2880

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/00837

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications.*) :

Description, pages:

1-15 version initiale

Revendications, N°:

1-13 version initiale

2. Les modifications ont entrainé l'annulation :

☐ de la description, pages :

☐ des revendications, n°s :

☐ des dessins, feuilles :

3. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

4. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-13
	Non :	Revendications	
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-13
Possibilité d'application industrielle	Oui :	Revendications	1-13
	Non :	Revendications	

2. Citations et explications

voir feuille séparée

Concernant le point V
Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'objet de la revendication 1 se distingue de l'art antérieur connu du document D1 (WO-A-8902140) uniquement par le fait qu'une **pluralité** de commandes de modifications sont appliquées par le terminal à la carte.
Le document D1, qui est cité dans la description de la présente demande à la page 1, lignes 27 - 30, ne prévoit l'application que d'une seule commande de modification à la fois. Plus précisément D1 a pour but de n'autoriser le débit de la carte que lorsque le service payé (connections téléphoniques) est vraiment fourni.
Le procédé connu de D1 ne prévoit la modification que d'une seule donnée de la carte.
L'objet de la revendication 1 est donc neuf.

Néanmoins, un homme de métier connaissant le procédé décrit par D1 et désirant l'appliquer à un système de télébillétique tout en conservant pour l'usager l'assurance que le paiement ne sera effectué que si le service est rendu (le ticket crédité sur la carte) va automatiquement et sans aucune activité inventive augmenter le nombre de commandes de modifications qui doivent être appliquées par le terminal à la carte vu que, par définition même de la télébillétique, la carte doit subir au moins deux modifications, débit du crédit et inscription du ticket.
Par conséquent l'homme de métier par simple adaptation de l'enseignement du document D1 à une utilisation de télébillétique va automatiquement arriver à l'objet de la revendication 1.

La revendication 1 ne remplit donc pas les dispositions de l'Art. 33 PCT car son objet ne présente aucune activité inventive.

L'examinateur est d'avis que l'objet de toutes les revendications dépendantes 2 à 13 découlent de façon évidente de l'application du procédé connu de D1 à un système de télébillétique. Par exemple, dans une utilisation télébillétique la création de certificat ou d'authentification est nécessaire et par conséquent évidente (voir revendications 5 - 10).

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 464-I51177WO	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 99/ 00837	Date du dépôt international *(jour/mois/année)* 09/04/1999	(Date de priorité (la plus ancienne) *(jour/mois/année)* 09/04/1998
Déposant INNOVATRON ELECTRONIQUE (SOCIETE ANONYME) et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

[ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

[ ] contenu dans la demande internationale, sous forme écrite.

[ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

[ ] remis ultérieurement à l'administration, sous forme écrite.

[ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

[ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

[ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

[X] le texte est approuvé tel qu'il a été remis par le déposant.

[ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé,**

[X] le texte est approuvé tel qu'il a été remis par le déposant

[ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° --

[ ] suggérée par le déposant.

[ ] parce que le déposant n'a pas suggéré de figure.

[ ] parce que cette figure caractérise mieux l'invention.

[ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 99/00837

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 89 02140 A (MARS) 9 mars 1989 (1989-03-09) cité dans la demande	1,2,12
A	abrégé; revendications; figures page 13, ligne 11 - page 20, ligne 6	5,6,8,9
Y	US 4 877 945 A (K. FUJISAKI) 31 octobre 1989 (1989-10-31) cité dans la demande le document en entier	1,2,12
A	DE 44 39 266 A (SIEMENS) 11 avril 1996 (1996-04-11) abrégé; revendications; figure	1-3,5,6, 8,10,12
A	FR 2 701 578 A (GEMPLUS CARD INTERNATIONAL) 19 août 1994 (1994-08-19)	

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
19 août 1999	27/08/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
P,A	FR 2 757 661 A (GEMPLUS) 26 juin 1998 (1998-06-26) abrégé; revendications; figures	1,2,5-7, 12
A	FR 2 689 662 A (GEMPLUS CARD INTERNATIONAL) 8 octobre 1993 (1993-10-08)	
A	EP 0 740 268 A (FRANCE TELECOM) 30 octobre 1996 (1996-10-30)	
A	EP 0 700 023 A (KONINKLIJKE PTT NEDERLAND) 6 mars 1996 (1996-03-06)	

1

INTERNATIONAL SEARCH REPORT

[redacted]ation on patent family members

[redacted]national Application No
PCT/FR 99/00837

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 8902140 A	09-03-1989	EP 0389484 A	03-10-1990
		JP 3501302 T	22-03-1991
US 4877945 A	31-10-1989	JP 63120391 A	24-05-1988
DE 4439266 A	11-04-1996	AT 163786 T	15-03-1998
		WO 9610810 A	11-04-1996
		DE 59501580 D	09-04-1998
		EP 0783741 A	16-07-1997
		ES 2113754 T	01-05-1998
		JP 9512368 T	09-12-1997
		US 5889266 A	30-03-1999
FR 2701578 A	19-08-1994	NONE	
FR 2757661 A	26-06-1998	WO 9828719 A	02-07-1998
FR 2689662 A	08-10-1993	NONE	
EP 0740268 A	30-10-1996	FR 2733615 A	31-10-1996
		JP 8305812 A	22-11-1996
		US 5767504 A	16-06-1998
		US 5847374 A	08-12-1998
EP 0700023 A	06-03-1996	NL 9401406 A	01-04-1996
		US 5635695 A	03-06-1997

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 99/00837

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 89 02140 A (MARS) 9 mars 1989 (1989-03-09) cité dans la demande	1,2,12
A	abrégé; revendications; figures page 13, ligne 11 - page 20, ligne 6	5,6,8,9
Y	US 4 877 945 A (K. FUJISAKI) 31 octobre 1989 (1989-10-31) cité dans la demande le document en entier	1,2,12
A	DE 44 39 266 A (SIEMENS) 11 avril 1996 (1996-04-11) abrégé; revendications; figure	1-3,5,6, 8,10,12
A	FR 2 701 578 A (GEMPLUS CARD INTERNATIONAL) 19 août 1994 (1994-08-19)	

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
19 août 1999	27/08/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 99/00837

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
P,A	FR 2 757 661 A (GEMPLUS) 26 juin 1998 (1998-06-26) abrégé; revendications; figures	1,2,5-7, 12
A	FR 2 689 662 A (GEMPLUS CARD INTERNATIONAL) 8 octobre 1993 (1993-10-08)	
A	EP 0 740 268 A (FRANCE TELECOM) 30 octobre 1996 (1996-10-30)	
A	EP 0 700 023 A (KONINKLIJKE PTT NEDERLAND) 6 mars 1996 (1996-03-06)	

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR 99/00837

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 8902140	A	09-03-1989	EP	0389484 A	03-10-1990
			JP	3501302 T	22-03-1991
US 4877945	A	31-10-1989	JP	63120391 A	24-05-1988
DE 4439266	A	11-04-1996	AT	163786 T	15-03-1998
			WO	9610810 A	11-04-1996
			DE	59501580 D	09-04-1998
			EP	0783741 A	16-07-1997
			ES	2113754 T	01-05-1998
			JP	9512368 T	09-12-1997
			US	5889266 A	30-03-1999
FR 2701578	A	19-08-1994	AUCUN		
FR 2757661	A	26-06-1998	WO	9828719 A	02-07-1998
FR 2689662	A	08-10-1993	AUCUN		
EP 0740268	A	30-10-1996	FR	2733615 A	31-10-1996
			JP	8305812 A	22-11-1996
			US	5767504 A	16-06-1998
			US	5847374 A	08-12-1998
EP 0700023	A	06-03-1996	NL	9401406 A	01-04-1996
			US	5635695 A	03-06-1997

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 556328
FR 9804453

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y A	WO 89 02140 A (MARS) 9 mars 1989 * abrégé; revendications; figures * * page 13, ligne 11 - page 20, ligne 6 *	1,2,12 5,6,8,9
Y	US 4 877 945 A (K. FUJISAKI) 31 octobre 1989 * le document en entier *	1,2,12
A	DE 44 39 266 A (SIEMENS) 11 avril 1996 * abrégé; revendications; figure *	1-3,5,6, 8,10,12
A	FR 2 701 578 A (GEMPLUS CARD INTERNATIONAL) 19 août 1994	
A	FR 2 689 662 A (GEMPLUS CARD INTERNATIONAL) 8 octobre 1993	
A	EP 0 740 268 A (FRANCE TELECOM) 30 octobre 1996	
A	EP 0 700 023 A (KONINKLIJKE PTT NEDERLAND) 6 mars 1996	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07F

Date d'achèvement de la recherche	Examinateur
9 mars 1999	David, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

ANNEXE AU RAPPORT DE RECHERCHE PRELIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO.

FA 556328
FR 9804453

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

09-03-1999

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 8902140 A	09-03-1989	EP 0389484 A	03-10-1990
		JP 3501302 T	22-03-1991
US 4877945 A	31-10-1989	JP 63120391 A	24-05-1988
DE 4439266 A	11-04-1996	AT 163786 T	15-03-1998
		WO 9610810 A	11-04-1996
		DE 59501580 D	09-04-1998
		EP 0783741 A	16-07-1997
		ES 2113754 T	01-05-1998
		JP 9512368 T	09-12-1997
FR 2701578 A	19-08-1994	AUCUN	
FR 2689662 A	08-10-1993	AUCUN	
EP 0740268 A	30-10-1996	FR 2733615 A	31-10-1996
		JP 8305812 A	22-11-1996
		US 5767504 A	16-06-1998
		US 5847374 A	08-12-1998
EP 0700023 A	06-03-1996	NL 9401406 A	01-04-1996
		US 5635695 A	03-06-1997

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/10 — A1

(11) Numéro de publication internationale: **WO 99/53451**

(43) Date de publication internationale: 21 octobre 1999 (21.10.99)

(21) Numéro de la demande internationale: PCT/FR99/00837

(22) Date de dépôt international: 9 avril 1999 (09.04.99)

(30) Données relatives à la priorité:
98/04453 9 avril 1998 (09.04.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: INNOVATRON ELECTRONIQUE, SOCIETE ANONYME [FR/FR]; 1, rue Danton, F-75006 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(US seulement)*: DIDIER, Stéphane [FR/FR]; 113, rue de Meaux, F-75019 Paris (FR). GRIEU, François [FR/FR]; 8, rue de Rambouillet, F-75012 Paris (FR).

(74) Mandataire: DUPUIS-LATOUR, Dominique; Cabinet Bardehle, Pagenberg & Partner, 14, boulevard Malesherbes, F-75008 Paris (FR).

(81) Etats désignés: AE, AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, SL, TR, TT, UA, UG, US, UZ, VN, YU, ZA, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: METHOD FOR INDIVISIBLY MODIFYING A PLURALITY OF SITES IN A MICROCIRCUIT CARD NON VOLATILE MEMORY, IN PARTICULAR A CONTACTLESS CARD

(54) Titre: PROCEDE POUR MODIFIER DE MANIERE INDIVISIBLE UNE PLURALITE D'EMPLACEMENTS DE LA MEMOIRE NON VOLATILE D'UNE CARTE A MICROCIRCUIT, NOTAMMENT UNE CARTE SANS CONTACT

(57) Abstract

The card is temporarily connected to a terminal while a transaction is being executed comprising the application by the terminal to the card of a plurality of modification commands each comprising at least an operation for posting, in the card memory, a respective information indicated by the command, the different data being thus posted mutually interdependent. Said method comprises the following steps executed by the card: a) on receiving from the terminal the corresponding respective modification commands, modifying the card memory content by provisional posting, in the card memory, each of said interdependent data without losing previous values corresponding to said data; then b) finalising said modifications, either by confirming all of them, or by denying them, such that for subsequent operations the commands executed at step a) are either all taken into account, or are all null and void.

(57) Abrégé

La carte est couplée temporairement à un terminal pendant l'exécution d'une transaction comportant l'application par le terminal à la carte d'une pluralité de commandes de modifications comprenant chacune au moins une opération d'inscription, dans la mémoire de la carte, d'une information respective désignée par la commande, les différentes informations ainsi inscrites étant mutuellement interdépendantes. Ce procédé comprend l'exécution par la carte des étapes suivantes: a) sur réception de commandes respectives correspondantes reçues du terminal, modifications du contenu de la mémoire de la carte par inscription provisoire, dans la mémoire de la carte, de chacune desdites informations interdépendantes sans perte de valeurs antérieures correspondant à ces informations; puis b) finalisation de ces modifications, soit en les confirmant toutes, soit en les infirmant toutes, de sorte que pour des opération ultérieures les commandes exécutées à l'étape a) soient soit toutes prises en compte, soit toutes sans effet.

Documents
>> Questel Plus
WPIL
1 - ep740268,fr2689662,fr2757661,fr2701578,de4439266/PN/XPN - 5
Doc. 1-5 de qu 1 depuis WPIL au format MAX

1/5 *WPIL*

Titre
Secure transmission of data over communication network - uses digital signatures stored in smart card, erasing signature when transfer is complete, and using presence or absence of signature to determine state of transfer

Données de publication

N° publication
FR2757661 A1 19980626 DW1998-32 G06K-019/073 25p * AP: 1996FR-0015980 19961224
WO9828719 A1 19980702 DW1998-32 G07F-007/08 Fre AP: 1997WO-FR02414 19971223 DSNW: JP SG US DSRW: AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
US6058483 A 20000502 DW2000-29 G06F-017/60 FD: Based on WO9828719 AP: 1997WO-FR02414 19971223; 1998US-0125664 19980914
N° priorité *1996FR-0015980 19961224*
Nb. pays couverts *20*
Nb. publications *3*
Termes supp. *GSM INTERNET*
CIB *G06F-017/60 G06K-019/073 G07F-007/08 G06K-005/00 H04K-001/00 H04L-009/00 H04L-009/32 H04L-*

Résumé

Basic
FR2757661 A The secure data transfer between a smart card and another device makes use of digital signatures to validate the initiation of the transfer of data, storing the signature in a memory zone in the smart card , then, when the transfer is complete, erasing the signature from the smart card memory.
The presence or absence of the digital signature in the card memory is used to determine whether the communication has stalled or has successfully completed. If the communication has stalled the digital signature in the card is replaced with a new, different, signature, and the communication resumed, with the new signature being removed when the transfer is terminated.
USE - Data transfer over cellular system such as GSM or over Internet
ADVANTAGE - Overcomes desynchronisation effects caused by interruption of communication between smart card and central computer. (Dwg.2/5)

Equiv. US
US6058483 A The secure data transfer between a smart card and another device makes use of digital signatures to validate the initiation of the transfer of data, storing the signature in a memory zone in the smart card , then, when the transfer is complete, erasing the signature from the smart card memory.
The presence or absence of the digital signature in the card memory is used to determine whether the communication has stalled or has successfully completed. If the communication has stalled the digital signature in the card is replaced with a new, different, signature, and the communication resumed, with the new signature being removed when the transfer is terminated.
USE - Data transfer over cellular system such as GSM or over Internet
ADVANTAGE - Overcomes desynchronisation effects caused by interruption of communication between smart card and central computer.

Déposant & Inventeur(s)
Déposant *(GEMP-) GEMPLUS SCA*
Inventeur(s) *VANNEL P*

Codes d'accès
Codes

2/5 *WPIL*

Données de publication

N° publication
EP-740268 A1 19961030 DW1996-48 G06K-019/073 Fre 12p * AP: 1996EP-0400867 19960424 DSR: DE GB NL
FR2733615 A1 19961031 DW1997-01 G06K-019/073 AP: 1995FR-0004992 19950426
JP08305812 A 19961122 DW1997-06 G06K-017/00 10p AP: 1996JP-0108205 19960426
US5767504 A 19980616 DW1998-31 G06K-019/06 AP: 1996US-0639268 19960424
US5847374 A 19981208 DW1999-05 G06K-019/06 FD: Div ex US5767504 AP: 1996US-0639268 19960424; 1997US-0985141 19971204
N° priorité *1995FR-0004992 19950426*
Nb. pays couverts *6*
Nb. publications *5*
Brevets cités *FR2689662; FR2698486; FR2701578*
CIB *G06K-017/00 G06K-019/06 G06K-019/073 G07F-007/10 G11C-005/00 G11C-016/06 H04M-015/00 H04M-*

Résumé

Basic

EP-740268 A The memory card comprises a counter region consisting of at least two levels of counters of at least two bits each which may be used on an abacus principle. A first indicator region consists of at least two indicast two bits, serving to display the effective erasure of the counters. There is also a balance region accessible for reading and writing. It is only erasable if the contents of the counter region have been incremented.

A second indicator region is structured in two fields associated with the balance region. Writing of the balance bits takes place simultaneously in the balance region and in the second indicator region. The balance region and the second indicator region each comprise a validation bit allowing determination of whether the present balance is completely written.

USE - Memory card for holding telephone call units enabling use of public telephone. (Dwg.2/2)

Déposant & Inventeur(s)

Déposant *(ETFR) FRANCE TELECOM*

Inventeur(s) *MŒNCONI M*

Codes d'accès

Codes

3/5 *WPIL*

Titre

Data transmission system incorporating non-volatile memory chip card - has two stored-value counters of which only one can be activated in non-volatile state while other serves as provisional counter

Données de publication

N° publication

DE4439266 A1 19960411 DW1996-20 G06K-019/10 7p * AP: 1994DE-4439266 19941103

WO9610810 A1 19960411 DW1996-21 G07F-007/08 Ger 23p AP: 1995WO-DE01286 19950919 DSNW: CN FI JP KR RU UA US DSRW: AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE

EP-783741 A1 19970716 DW1997-33 G07F-007/08 Ger FD: Based on WO9610810 AP: 1995EP-0931886 19950919; 1995WO-DE01286 19950919 DSR: AT CH DE ES FR GB IT LI

JP09512368 W 19971209 DW1998-08 G06F-019/00 19p FD: Based on WO9610810 AP: 1995WO-DE01286 19950919; 1996JP-0511263 19950919

EP-783741 B1 19980304 DW1998-13 G07F-007/08 Ger 11p FD: Based on WO9610810 AP: 1995EP-0931886 19950919; 1995WO-DE01286 19950919 DSR: AT CH DE ES FR GB IT LI

DE59501580 G 19980409 DW1998-20 G07F-007/08 FD: Based on EP-783741; Based on WO9610810 AP: 1995DE-5001580 19950919; 1995EP-0931886 19950919; 1995WO-DE01286 19950919

ES2113754 T3 19980501 DW1998-24 G07F-007/08 FD: Based on EP-783741 AP: 1995EP-0931886 19950919

KR97706557 A 19971103 DW1998-44 G07F-007/08 FD: Based on WO9610810 AP: 1995WO-DE01286 19950919; 1997KR-0702002 19970327

US5889266 A 19990330 DW1999-20 G06K-005/00 AP: 1995WO-DE01286 19950919; 1997US-0828720 19970331

RU2134904 C1 19990820 DW2000-32 G07F-007/08 FD: Based on WO9610810 AP: 1995WO-DE01286 19950919; 1997RU-0106803 19950919

N° priorité *1994DE-4435137 19940930*

Nb. pays couverts *24*

Nb. publications *10*

Brevets cités *DE4230866; EP-268106; EP-292658; EP-398545; EP-409701; FR2667192; FR2689662; FR2701578*

CIB *G06F-019/00 G06K-005/00 G06K-019/10 G07F-007/08 G06F-007/08 G06F-012/14 G06F-012/16 G06K-0-*

Résumé

Basic

DE4439266 A The card inserted into a recharging terminal carries a nonvolatile semiconductor memory (NVM) e.g. an EEPROM divided into areas including two multistage counters (WBA,WBB) linked by a switching device (SV) to programming logic (PL) and verification logic (VL) in a control unit (ST).

The switching is performed by a selection logic circuit (AL) connected to a nonvolatile flag memory (FS) and addressed by a charging control signal (LAD). The new count is written into the provisional counter which is switched into the nonvolatile state only after a check on correct writing.

USE/ADVANTAGE - For reloadable phonecard as counter for prepaid units. Counter of portable data carrier can be recharged easily without risk of fraudulent manipulation because of swapping between volatile and non-volatile memory.(Dwg.1/1)

Equiv. Europ.

EP-783741 B The card inserted into a recharging terminal carries a nonvolatile semiconductor memory (NVM) e.g. an EEPROM divided into areas including two multistage counters (WBA,WBB) linked by a switching device (SV) to programming logic (PL) and verification logic (VL) in a control unit (ST).

The switching is performed by a selection logic circuit (AL) connected to a nonvolatile flag memory (FS) and addressed by a charging control signal (LAD). The new count is written into the provisional counter which is switched into the nonvolatile state only after a check on correct writing.

USE/ADVANTAGE - For reloadable phonecard as counter for prepaid units. Counter of portable data carrier can be

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

Procédé pour modifier de manière indivisible une pluralité d'emplacements de la mémoire non volatile d'une carte à microcircuit, notamment une carte sans contact

L'invention concerne les cartes à microcircuit, et plus particulièrement les cartes à microprocesseur, qui réalisent elles-mêmes diverses modifications de leur mémoire non volatile.

Lors de l'exécution d'une transaction, la mémoire est généralement modifiée, une ou plusieurs fois, et il est bien entendu nécessaire de s'assurer alors que toutes les modifications ont bien été correctement effectuées avant de pouvoir exploiter les informations nouvellement inscrites, les informations nouvellement inscrites devant être ignorées ou effacées en cas d'erreur ou de défaut d'intégrité de l'inscription.

Le US-A-4 877 945 décrit ainsi la manière de détecter une anomalie survenue au cours d'une séquence d'écriture de plusieurs informations afin d'empêcher la poursuite de la transaction sur des bases erronées.

Il est par ailleurs souhaitable, en cas d'anomalie, de pouvoir revenir au *statu quo ante*, c'est-à-dire qu'une transaction ultérieure devra être à même d'opérer sur les valeurs des informations qui étaient inscrites dans la carte avant l'exécution de la transaction incorrecte.

Le US-A-4 877 945 précité n'offre pas cet avantage, car les anciennes valeurs des informations auront, pour certaines, été perdues pendant l'exécution de la transaction incorrecte, de sorte qu'il ne sera pas possible de restaurer ces informations à leur état antérieur, du moins à partir des seules informations contenues dans cette carte.

Le WO-A-89/02140, quant à lui, décrit une telle manière d'opérer, mais qui n'est applicable qu'au cas de la modification d'une information unique ou de plusieurs modifications d'informations indépendamment les unes de autres.

Dans de nombreux cas, il est cependant nécessaire de modifier au cours de la même transaction plusieurs informations, et elles seront considérées "mutuellement interdépendantes" si elles nécessitent d'être traitées ensemble pour la bonne exécution de l'ensemble des modifications de l'ensemble des informations.

Le risque de transaction imparfaite ou inachevée portant sur une pluralité d'informations interdépendantes est particulièrement élevé avec les cartes du type "sans contact", où les limites du volume dans lequel la carte peut fonctionner correctement autour du terminal ne sont pas perceptibles. Il existe dans ce cas un risque non négligeable de rupture inattendue de la communication entre carte et terminal, dû à la sortie de la carte du rayon d'action du terminal avant la fin du traitement, ou du fait d'une perturbation passagère, par exemple le passage d'une masse métallique à proximité.

Un exemple (bien entendu non limitatif) est l'utilisation d'une telle carte dans une transaction de télébillétique, c'est-à-dire pour l'accès à un réseau de transport public, la carte jouant le double rôle de titre de transport et de porte-monnaie électronique.

Pour pallier les difficultés précitées, et rendre "indivisibles" une pluralité d'écritures ou autres modifications de données interdépendantes, plusieurs solutions ont été proposées.

Dans l'exemple d'application indiqué plus haut, les systèmes connus commencent par débiter le porte-monnaie, puis inscrivent les droits de transport acquis par l'usager. Si l'usager retire sa carte entre les deux opérations, il est invité à présenter la carte à nouveau et l'écriture des droits de transport est reprise. En revanche, s'il part sans représenter sa carte, il aura été lésé. Il est bien évidemment impossible de procéder dans l'ordre inverse car l'usager aurait alors intérêt à retirer sa carte avant que le porte-monnaie ne soit débité.

Cette solution implique que le terminal soit spécialement configuré pour permettre, en cas d'interruption, l'activation d'un traitement d'exception gérant la reprise de la transaction (réinsertion de la carte sur demande du terminal). Outre la complexification du logiciel du terminal, cette solution n'est pas totalement satisfaisante dans la mesure où, comme on l'a indiqué, l'usager se trouve néanmoins lésé en cas de non-reprise de la transaction.

Une autre solution consiste à utiliser des informations croisées, en conservant dans le terminal des informations sur l'état du porte-monnaie de la carte, et réciproquement. Mais cette solution n'est pas non plus satisfaisante car, outre sa complexité, elle augmente le volume de

données échangées entre carte et terminal et ralentit donc l'exécution de la transaction. Elle est en outre difficilement applicable à un nombre important d'écritures à rendre indivisibles (trois et plus).

L'un des buts de l'invention est de proposer un procédé permettant d'effectuer une pluralité de modifications de la mémoire de la carte de manière indivisible.

Un autre but de l'invention est de proposer un tel procédé qui puisse être entièrement géré par la carte. Ce procédé pourra donc être mis en œuvre sans modification des terminaux et sans qu'il y ait lieu de prévoir des traitements d'exception par ces terminaux, en utilisant la syntaxe des ordres existants et donc avec une grande souplesse dans le choix des commandes.

Le procédé de l'invention est du type dans lequel la carte est couplée temporairement à un terminal pendant l'exécution d'une transaction comportant l'application par le terminal à la carte d'une pluralité de commandes de modifications comprenant chacune au moins une opération d'inscription, dans la mémoire de la carte, d'une information respective désignée par la commande, les différentes informations ainsi inscrites étant mutuellement interdépendantes.

De façon caractéristique de l'invention, ce procédé comprend l'exécution, par la carte, des étapes suivantes : a) sur réception de commandes respectives correspondantes reçues du terminal, modifications du contenu de la mémoire de la carte par inscription provisoire, dans la mémoire de la carte, de chacune desdites informations interdépendantes sans perte de valeurs antérieures correspondant à ces informations ; puis b) finalisation de ces modifications, soit en les confirmant toutes, soit en les infirmant toutes, de sorte que pour des opérations ultérieures les commandes exécutées à l'étape a) soient soit toutes prises en compte, soit toutes sans effet.

Le principe de base de l'invention consiste ainsi à grouper la pluralité de modifications à réaliser de manière indivisible au sein d'une même étape a) et, après avoir exécuté ces modifications, à valider globalement ces modifications par la carte. Si la validation est effective, à la prochaine opération effectuée par la carte (au cours de la même transaction ou au cours d'une transaction ultérieure), son contenu accessi-

ble reflétera nécessairement les modifications opérées.

Inversement, toute interruption du fonctionnement de la carte intervenant au cours de l'étape a) annulera l'ensemble des modifications effectuées, et les données de la mémoire non volatile resteront dans leur état antérieur à l'étape a).

Dans un mode de réalisation particulier, en cas de confirmation à l'étape b), on inscrit dans la mémoire de la carte un témoin confirmatif de bonne exécution et, lorsque la carte reçoit ultérieurement une commande impliquant la lecture et/ou la modification de l'une au moins des informations inscrites à l'étape a) ou de la valeur y correspondant, la carte examine préalablement l'état du témoin et, si celui-ci n'a pas été inscrit, la carte ignore ou annule les inscriptions provisoires antérieurement opérées à l'étape a) et exécute la commande sur la base desdites valeurs antérieures correspondant aux informations. Lorsque la carte examine l'état du témoin, si celui-ci a été inscrit la carte peut alors exécuter des opérations de recopie des écritures provisoires opérées à l'étape a).

Très avantageusement, la carte est apte à fonctionner selon deux modes, à savoir un mode en session, dans lequel les inscriptions sont opérées par exécution des étapes a) et b), et un mode hors session, dans lequel l'opération des inscriptions n'est pas confirmée à l'ensemble des étapes a) et b).

L'ouverture de session peut être implicite, par exemple à la remise à zéro (reset) de la carte ou suite à une commande à double action d'exécution d'une opération prédéterminée et interprétée comme un ordre d'ouverture de session.

Par exemple, quand une inscription normalement certifiée n'est pas accompagnée d'un certificat, la carte ouvre automatiquement une session qui traite l'inscription dans cette session.

De la même façon, la fermeture de session peut être implicite, suite à une commande à double action d'exécution d'une opération prédéterminée et interprétée comme un ordre de fermeture de session.

Par exemple, une opération de débit du porte-monnaie ferme la session, ce qui de plus évite de devoir différer la communication du certificat résultant et permet de confondre les certificats de session avec

ceux de transaction du porte-monnaie.

Très avantageusement, le procédé comprend une fonction d'authentification combinée à la fonction de finalisation de l'étape b), forçant l'infirmation à l'étape b) dans le cas où l'authentification échoue.

Dans une première mise en œuvre, cette authentification est opérée par la carte qui authentifie le terminal et/ou les données échangées entre terminal et carte, la carte contrôlant un certificat cryptographique produit par le terminal et transmis à la carte et ne confirmant les modifications à l'étape b) que si ce certificat est reconnu correct.

Dans le cas d'un mode avec session, on peut prévoir que, lorsque la carte reçoit du terminal des commandes de modification du contenu de la mémoire incluant la vérification d'un certificat cryptographique, cette vérification est opérée si la commande est reçue hors session, et ne l'est pas si la commande est reçue en session.

En d'autres termes, celles des commandes exécutées par la carte b) à l'étape b) qui normalement (c'est-à-dire hors session) vérifieraient un certificat cryptographique, ne comprennent plus cette vérification quand elles sont exécutées dans le cadre d'une session, le "certificat de session authentifiant le terminal" réalisant une fonction équivalente.

Dans une seconde mise en œuvre, l'authentification est opérée par le terminal qui authentifie la carte et/ou les données échangées entre terminal et carte, la carte produisant et transmettant au terminal un certificat cryptographique de manière conditionnelle, si et seulement si les modifications ont été confirmées à l'étape b).

Dans le cas d'un mode avec session, on peut prévoir que, lorsque la carte reçoit du terminal à l'étape b) des commandes de modification du contenu de la mémoire incluant la production d'un certificat cryptographique, cette production est opérée si la commande est reçue hors session, et ne l'est pas si la commande est reçue en session.

En d'autres termes, celles des commandes exécutées par la carte à l'étape b) qui normalement (c'est-à-dire hors session) produiraient un certificat cryptographique, ne comprennent plus cette production quand elles sont exécutées dans le cadre d'une session, le "certificat de session authentifiant le terminal" réalisant une fonction équivalente.

On peut par ailleurs prévoir que, lorsque la carte reçoit du terminal

des commandes de modification du contenu de la mémoire incluant la production d'une pluralité de certificats cryptographiques, ces certificats sont mémorisés à cette étape b), puis transmis ensemble au terminal si et seulement si les modifications ont été confirmées à l'étape b).

En d'autres termes, on prévoit de différer la communication par la carte des certificats cryptographiques produits normalement par les ordres de l'étape b). En particulier, si une commande d'écriture certifiée produit un certain certificat d'écriture, il est souhaitable que celui-ci ne sorte de la carte qu'une fois l'écriture effectuée irrévocablement.

Dans une forme de mise en œuvre particulière, au moins certaines des commandes susceptibles d'être exécutées à l'étape b) comprennent un éventuel attribut d'inhibition et, si la carte exécute une telle commande en session à une étape b), les modifications opérées par cette commande prennent effet indépendamment du résultat de l'étape b).

En d'autres termes, l'attribut définit si la commande est effectuée en session (c'est-à-dire sera annulée si la session n'est pas fermée) ou hors session (c'est-à-dire effective immédiatement, comme si elle était effectuée hors session, même si elle est chronologiquement en session).

Très avantageusement, le procédé prévoit en outre, après l'étape b) et en cas de confirmation des modifications, la séquence d'étapes suivante : d) exécution par le terminal d'une action suite à la confirmation par la carte ; e) en cas de bonne exécution de ladite action par le terminal, inscription dans la carte d'une information de ratification ultérieurement accessible en lecture.

Une telle "ratification" de la session indique à la carte que le terminal a effectivement pu prendre les décisions (par exemple l'ouverture d'un portillon dans le cas d'une application d'accès à un réseau de transport en commun) suite à l'exécution de la session.

On notera que cette ratification est gérée par la carte sans nécessité d'une écriture supplémentaire (la recopie des écritures provisoires étant une opération qui, de toute façon, doit être tôt ou tard effectuée). En outre cette recopie n'est opérée côté carte qu'à condition que l'action est bien exécutée côté terminal, c'est-à-dire uniquement en cas de cohérence de l'ensemble de la transaction.

L'ensemble des opérations étant gérée par la carte, on peut avanta-

geusement prévoir que la commande d'inscription de l'étape e) est une commande implicite, toute commande reçue par la carte après l'étape b) étant interprétée comme un ordre d'inscription dans la carte d'une information de ratification.

D'autres caractéristiques et avantages ressortiront de la description ci-dessous de deux exemples de mise en œuvre de l'invention.

Dans ces exemples, comme d'ailleurs dans le reste du texte, le mot "désigner", ici entendu au sens de "déterminer un parmi plusieurs", vise l'action consistant à caractériser une information particulière parmi les différentes informations contenues dans la carte.

Cette désignation peut être implicite, parce que la commande vise par elle-même une information particulière ; par exemple, la commande "débiter le porte-monnaie d'un montant x" désigne l'emplacement mémoire contenant la valeur de l'information "solde du porte-monnaie".

Elle peut être également explicite, comme par exemple dans l'exemple I ci-dessous, où il est prévu des commandes d'écriture avec une adresse ou un identifiant de secteur, indexés par un indice i.

Exemple I

On se propose de réaliser une carte stockant 100 valeurs de huit octets chacune, et supportant les ordres :

— Lecture d'une valeur v de 8 octets, désignée par son indice i de 1 à 100.
— Écriture d'une valeur v de 8 octets, désignée par son indice i de 1 à 100.
— Ouverture de session.
— Fermeture de session.

La carte doit permettre jusqu'à trois écritures dans une même session. Par convention, on utilisera des lettres majuscules pour désigner les valeurs en mémoire non volatile (EEPROM par exemple) et des lettres minuscules pour désigner les valeurs en mémoire volatile (RAM, dont le contenu est perdu à la mise hors tension).

Une zone de mémoire non volatile est affectée au stockage principal

des données de la carte (écritures définitives) :

- V[i], i de 1 à 100 : 100 x 8 octets

Une autre zone de mémoire non volatile est affectée au mécanisme de session, et comprend :

- T[k], j de 1 à 3 : 3 x 8 octets contenant les valeurs écrites pendant la session (écritures provisoires).
- I[k], j de 1 à 3 : 3 x 1 octet contenant les indices des valeurs écrites pendant la session.
- C : 1 octet de comptage qui sera écrit en fin de session.

C code le nombre d'écritures effectuées dans la session ; un mécanisme de redondance approprié (associant par exemple le complément de cette valeur) permet d'assurer que l'on sait détecter le cas où la valeur stockée dans cet octet de comptage est incertaine.

Le déroulement des opérations est le suivant.

Étape 0 : à un moment compris entre la mise sous tension de la carte et la première commande réalisée, C est examiné. S'il est à une valeur certaine de 1 à 3, alors pour k de 1 à C on copie la valeur T[k] à l'indice I[k] du tableau V[i]. Puis C est mis à 0, et une variable interne j à -1 (pour indiquer qu'une session n'est pas ouverte).

Étape 1 : à la lecture on examine si j>0; si oui, on compare l'indice i demandé avec les valeurs I[k] pour k de j à 1 en décroissant. En cas d'identité, on retourne T[k]. Dans tous les autres cas, on retourne V[i].

Étape 2 : à l'ouverture de session, on initialise j = 0 (à noter que si une session est ouverte, elle est annulée)

Étape 3 : à chaque écriture, si j =-1 (session non ouverte), on écrit la valeur v communiquée en T[0], l'indice i communiqué en I[0], puis on écrit C=1, puis on écrit v en V[i], puis on écrit C=0; si $0 \leq j < 3$ (écriture en session), on augmente j de 1, on écrit v en T[j], on écrit i en I[j]; si j=3 on refuse l'opération (dépassement de la limite des écritures en session).

Étape 4 : à la fermeture de session, si j>0, on écrit j en C, puis pour j de 1 à C on copie la valeur T[j] à l'indice I[j] du tableau V[]. Puis C est mis à 0, et j à -1.

On montre qu'à tout moment on peut couper l'alimentation de la carte et que les valeurs lues seront correctes, c'est-à-dire pour chaque indice i la dernière valeur écrite hors session ou écrite dans une session close (l'écriture est achevée ou la session est close au moment où une valeur non nulle est écrite dans C).

La cryptographie s'ajoute en empêchant certaines opérations si un certificat cryptographique fourni à la carte est incorrect, et/ou en faisant produire à la carte des certificats cryptographiques à l'issue de certaines opérations.

Les certificats cryptographiques utilisés sont basés sur une cryptographie de type connu. Par exemple, le "certificat de session authentifiant la carte" (respectivement, le terminal) est obtenu en appliquant côté carte et terminal l'algorithme *Secure Hash Algorithm* (SHA) aux données fournies par la carte (resp. le terminal) et à un nombre aléatoire fourni par le terminal (resp. la carte) à l'ouverture de la session ; le *Message Authentication Code* (MAC) résultant est signé par la carte (resp. le terminal) par l'algorithme de signature *Digital Signature Algorithm* (DSA) avec une clé secrète contenue dans la carte (resp. le terminal) ; le terminal (resp. la carte) vérifie cette signature avec une clé publique. Un algorithme de cryptographie symétrique tel que *Data Encryption Standard* (DES) peut aussi être utilisée pour la production du MAC et/ou l'élaboration des signatures.

Selon une option de l'invention, l'étape de production du MAC est commune aux deux sens d'authentification, et porte sur l'ensemble des données de la session. Et dans le cas d'une cryptographie symétrique, le certificat authentifiant la carte et celui authentifiant le terminal sont obtenus par une seule étape de chiffrement du MAC, les certificats respectifs de la carte et du terminal s'en déduisant par une opération élémentaire telle qu'extraction de certains bits prédéterminés.

Exemple II

Dans cet exemple les données de la mémoire sont organisées en secteurs comportant chacun quatre champs :

1. données ;
2. identifiant (clé d'accès permettant de sélectionner un secteur) ;
3. pertinence : permet de déterminer le secteur pertinent si deux secteurs ont le même identifiant ;
4. contrôle : permet de vérifier l'intégrité des trois champs précédents (par exemple un contrôle de type parité).

Un secteur sera désigné par son identifiant, notion qui se substitue à celle d'adresse. La procédure d'écriture d'un secteur a comme paramètre un identifiant et des données à associer à cet identifiant. La procédure de lecture d'un secteur a comme paramètre un identifiant, et retourne les données associées à cet identifiant lors de la dernière écriture effectuée avec ce même identifiant (ou une indication appropriée si cet identifiant n'a jamais été utilisé). En d'autres termes, on réalise un accès de type associatif au lieu d'un accès indexé.

Lors de la procédure de lecture d'un secteur, la carte recherche les secteurs dont l'identifiant a la valeur demandée, et qui (sur la base du champ de contrôle) sont intègres. Au cas où plusieurs secteurs répondent à ces deux critères, elle en retient un sur la base du champ de pertinence.

Lors d'une écriture de secteur, la carte écrit, dans un secteur disponible, les champs données et identifiant demandés, le champ pertinence tel que ce secteur sera, pour la procédure de lecture, le plus pertinent des secteurs intègres possédant cet identifiant, et le champ contrôle en accord avec les trois champs précédents (en d'autres termes, l'écriture est gérée de manière que la lecture ultérieure puisse être correctement opérée).

Avantageusement, la procédure d'écriture se poursuit par l'effacement du secteur rendu non pertinent par l'écriture du nouveau secteur, créant ainsi un nouveau secteur disponible.

On prévoit avantageusement un système (complémentaire) de type *garbage collection*, c'est-à-dire de récupération des secteurs inutiles, qu'ils soient non intègres ou non pertinents.

On prévoit avantageusement un système qui répartit l'usure résultant de l'écriture en évitant d'utiliser toujours les mêmes secteurs, par

exemple en choisissant aléatoirement un secteur parmi les secteurs disponibles.

Une variante généralement avantageuse de la procédure de recherche de secteur consiste à profiter de cette étape de recherche pour effacer les secteurs dont il est déterminé qu'ils sont non intègres, et/ou ceux qui ne sont pas les plus pertinents, recréant ainsi des secteurs libres (cela perd du temps lors de cette lecture, en faveur de la vitesse des lectures et écritures ultérieures). Avantageusement, avant l'effacement d'un secteur dont on a déterminé qu'il est intègre mais non pertinent, on écrira à nouveau le secteur pertinent, dont l'écriture peut être imparfaite.

La taille utile de la mémoire est égale au nombre de secteurs disponibles, moins un secteur qui doit rester effacé. Tous les secteurs (y compris celui effacé) sont répartis dynamiquement dans la mémoire.

Si les données doivent être structurées en fichiers, par exemple selon la norme ISO/IEC 7816-4, l'identifiant de secteur se décompose en deux sous-champs, un identifiant de fichier et un identifiant du secteur dans ce fichier.

On va donner ci-dessous une implémentation (non limitative) des opérations de lecture/écriture utilisant cette structuration particulière en secteurs :

— Le champ de contrôle contient, codé en binaire, le nombre de bits à zéro dans les trois autres champs ; on montre que si un problème tel qu'une écriture ou un effacement interrompu modifie un nombre quelconque de bits du secteur tous dans le même sens, le contrôle de la valeur du champ de contrôle permet toujours la détection du problème.
— Le champ pertinence est un entier de 0 à 3, codé sur 2 bits.
— La procédure de lecture parcourt séquentiellement tous les secteurs jusqu'à trouver un premier secteur possédant l'identifiant recherché, et intègre. Si cette recherche ne trouve aucun secteur, on termine la procédure avec un compte-rendu "secteur non trouvé". Si on trouve un tel premier secteur, on mémorise sa position, ses données, et sa pertinence p. La recherche se poursuit. Si l'on dé-

tecte un second secteur possédant l'identifiant recherché, et intègre, on teste si sa pertinence q est le reste de la division entière de p+1 par 3 ; si oui, on écrit à nouveau le second secteur, on efface le premier et on retourne les données du second ; sinon, on écrit à nouveau le premier secteur, on efface le second et on retourne les données du premier. Si un second secteur n'est pas trouvé et si la pertinence du premier secteur est p=3, on efface ce secteur et on donne le compte-rendu "secteur non trouvé" ; dans les autres cas, on retourne les données du premier secteur trouvé.

— La procédure d'écriture commence comme la procédure de lecture ci-dessus. Si l'on a trouvé le secteur que retournerait la procédure de lecture pour l'identifiant fourni, on mémorise la position de ce secteur et sa pertinence p (qui vaut 0, 1 ou 2) ; si on ne l'a pas trouvé, on sélectionne un secteur libre (par la procédure ci-après) et on écrit dans ce secteur les champs identifiant, données, pertinence p=3 et contrôle, et l'on mémorise la position et la pertinence de ce secteur. Dans les deux cas, on poursuit en sélectionnant un secteur libre (par la procédure ci-après). On écrit dans ce secteur les champs identifiant, données, pertinence q (calculée comme le reste de la division entière de p+1 par 3) et contrôle. Puis on efface le secteur mémorisé.

— Pour la recherche de secteur libre, on initialise à zéro le nombre n de secteurs libres trouvés. On examine séquentiellement les secteurs. Pour chaque secteur, s'il est non vierge et non intègre, on l'efface et il devient vierge (contribuant ainsi à la *garbage collection* mentionnée plus haut) ; s'il est intègre et si sa pertinence est p=3, on l'efface (idem) ; s'il est intègre et si sa pertinence n'est pas p=3, alors on recherche dans la zone non encore parcourue un autre secteur intègre de même identifiant, et si l'on en trouve un on efface celui qui n'est pas pertinent, en procédant comme pour la lecture ; si à l'issue de ce processus le secteur est vierge, on incrémente le nombre n de secteurs libres trouvés, et l'on effectue le tirage aléatoire d'un entier de 0 à n-1 ; si cet entier est 0, on mémorise la position du secteur vierge. Quand tous les secteurs ont été parcourus, tous les secteurs non vierges sont intègres, il n'existe pas deux

secteurs de même identifiant, on connaît le nombre n de secteurs vierges, et l'on a mémorisé l'un d'eux choisi aléatoirement de manière équiprobable. Si aucun secteur libre n'est trouvé, la procédure d'écriture est interrompue.

On va maintenant indiquer la manière dont la carte peut gérer des sessions de modifications indivisibles avec une telle structuration particulière en secteurs.

Pour stocker les modifications indivisibles, la carte dispose dans la mémoire non volatile de N secteurs effacés (N correspondant au nombre de modifications indivisibles que l'on pourra effectuer au cours d'une même session). De plus, elle gère une zone de la mémoire non volatile (hors secteurs) dédiée à la gestion de session et appelée "descripteur de session".

Cet exemple d'implémentation ne comprend aucune authentification propre à la session.

On définit un descripteur de session, composé de 3 champs :

— Liste des références des secteurs indivisibles (LRSA).

— Valeur de contrôle de création de la liste des références des secteurs indivisibles (VCC).

— Valeur de contrôle de prise en compte de la liste des références des secteurs indivisibles (VCPC), qui permettra de savoir si l'on a ou non fermé une session).

Étape 0 : initialisation : avant le premier accès aux données depuis la dernière interruption de fonctionnement de la carte, par exemple au *reset* (remise à zéro), la carte doit faire en sorte que le descripteur de session soit effacé. Il y a plusieurs cas à considérer, selon l'état du descripteur de session :

— Il est totalement effacé : la carte le laisse en l'état.

— Il n'est pas totalement effacé, et la VCPC est correcte : la carte recherche et efface (si nécessaire) tous les secteurs rendus obsolètes par ceux écrits (parmi ceux référencés dans la liste), puis efface le descripteur de session.

— Il n'est pas totalement effacé, la VCPC est effacée ou incorrecte et la VCC est correcte : la carte efface les secteurs indiqués dans

la LRSA, puis efface le descripteur de session.

— Il n'est pas totalement effacé, la VCPC est effacée ou incorrecte et la VCC est effacée ou incorrecte : la carte efface le descripteur de session.

Étape 1 : ouverture de session : la carte recherche N secteurs effacés, puis note la liste de leur référence et sa VCC dans le descripteur de session (supposé effacé).

Étape 2 : en cours de session : la carte reçoit des commandes. Lorsque l'une d'elle provoque une ou plusieurs modifications indivisibles, les secteurs utilisés pour noter ces modifications sont ceux notés dans la LRSA, à concurrence de N secteurs modifiés.

Étape 3 : fermeture de session : pour fermer la session, la carte écrit la VCPC, qui assure que la LRSA et sa VCC ont été pris en compte. Ensuite, elle recherche et efface tous les secteurs rendus obsolètes par ceux écrits (parmi ceux référencés dans la liste). Enfin, elle efface le descripteur de session.

Si, en outre, la carte gère la ratification, la gestion des sessions comporte les modifications ci-après.

Étape 0 : initialisation : dans ce lui des cas où le descripteur de session n'est pas totalement effacé et la VCPC est correcte, la carte recherche et efface (si nécessaire) tous les secteurs rendus obsolètes par ceux écrits (parmi ceux référencés dans la liste), mais elle n'efface pas le descripteur de session.

Étape 1 : ouverture de session : la carte note en mémoire volatile qu'une session est ouverte. Si le descripteur de session n'est pas vierge, la carte signale que la session précédente n'a pas été ratifiée et peut même, en analysant la LRSA, indiquer quelles sont les données non ratifiées. Quoiqu'il arrive, elle ne modifie pas le descripteur de session.

Étape 2 : en cours de session : lors de la première commande avec modifications indivisibles, la carte efface le descripteur de session si nécessaire, recherche N secteurs effacés, puis écrit la LRSA et sa VCC.

Étape 3 : fermeture de session : la carte note en mémoire volatile

qu'aucune session n'est ouverte. Quoiqu'il arrive, elle n'efface pas le descripteur de session.

REVENDICATIONS

1. Un procédé pour modifier le contenu de la mémoire non volatile d'une carte à microcircuit, notamment d'une carte sans contact,

procédé dans lequel la carte est couplée temporairement à un terminal pendant l'exécution d'une transaction, notamment d'une transaction de télébillétique, comportant l'application par le terminal à la carte d'une pluralité de commandes de modifications comprenant chacune au moins une opération d'inscription, dans la mémoire de la carte, d'une information respective désignée par la commande, les différentes informations ainsi inscrites étant mutuellement interdépendantes,

procédé caractérisé en ce qu'il comprend l'exécution, par la carte, des étapes suivantes :

a) sur réception de commandes respectives correspondantes reçues du terminal, modifications du contenu de la mémoire de la carte par inscription provisoire, dans la mémoire de la carte, de chacune desdites informations interdépendantes sans perte de valeurs antérieures correspondant à ces informations ; puis

b) finalisation de ces modifications, soit en les confirmant toutes, soit en les infirmant toutes, de sorte que pour des opérations ultérieures les commandes exécutées à l'étape a) soient soit toutes prises en compte, soit toutes sans effet.

2. Le procédé de la revendication 1, dans lequel :

— en cas de confirmation à l'étape b), on inscrit dans la mémoire de la carte un témoin confirmatif de bonne exécution, et

— lorsque la carte reçoit ultérieurement une commande impliquant la lecture et/ou la modification de l'une au moins des informations inscrites à l'étape a) ou de la valeur y correspondant, la carte examine préalablement l'état du témoin et, si celui-ci n'a pas été inscrit, la carte ignore ou annule les inscriptions provisoires antérieurement opérées à l'étape a) et exécute la commande sur la base desdites valeurs antérieures correspondant aux informations.

3. Le procédé de la revendication 2, dans lequel, lorsque la carte

examine l'état du témoin, si celui-ci a été inscrit la carte exécute des opérations de recopie des écritures provisoires opérées à l'étape a).

4. Le procédé de l'une des revendications 1 et 2, dans lequel la carte est apte à fonctionner selon deux modes, à savoir :

— un mode en session, dans lequel les inscriptions sont opérées par exécution des étapes a) et b), et
— un mode hors session, dans lequel l'opération des inscriptions n'est pas confirmée à l'ensemble des étapes a) et b).

5. Le procédé de l'une des revendications 1 à 4, comprenant une fonction d'authentification combinée à la fonction de finalisation de l'étape b), forçant l'infirmation à l'étape b) dans le cas où l'authentification échoue.

6. Le procédé de la revendication 5, dans lequel ladite authentification est opérée par la carte qui authentifie le terminal et/ou les données échangées entre terminal et carte, la carte contrôlant un certificat cryptographique produit par le terminal et transmis à la carte et ne confirmant les modifications à l'étape b) que si ce certificat est reconnu correct.

7. Le procédé des revendications 4 et 6 prises en combinaison, dans lequel, lorsque la carte reçoit du terminal des commandes de modification du contenu de la mémoire incluant la vérification d'un certificat cryptographique, cette vérification est opérée si la commande est reçue hors session, et ne l'est pas si la commande est reçue en session.

8. Le procédé de la revendication 5, dans lequel ladite authentification est opérée par le terminal qui authentifie la carte et/ou les données échangées entre terminal et carte, la carte produisant et transmettant au terminal un certificat cryptographique de manière conditionnelle, si et seulement si les modifications ont été confirmées à l'étape b).

9. Le procédé des revendications 4 et 8 prises en combinaison, dans

lequel, lorsque la carte reçoit du terminal des commandes de modification du contenu de la mémoire incluant la production d'un certificat cryptographique, cette production est opérée si la commande est reçue hors session, et ne l'est pas si la commande est reçue en session.

10. Le procédé de l'une des revendications 1 et 2, dans lequel, lorsque la carte reçoit du terminal à l'étape b) des commandes de modification du contenu de la mémoire incluant la production d'une pluralité de certificats cryptographiques, ces certificats sont mémorisés à cette étape b), puis transmis ensemble au terminal si et seulement si les modifications ont été confirmées à l'étape b).

11. Le procédé des revendications 1 et 4 prises en combinaison, dans lequel au moins certaines des commandes susceptibles d'être exécutées à l'étape b) comprennent un éventuel attribut d'inhibition, et dans lequel, si la carte exécute une telle commande en session à une étape b), les modifications opérées par cette commande prennent effet indépendamment du résultat de l'étape b).

12. Le procédé de l'une des revendications 1 et 2, dans lequel il est en outre prévu, après l'étape b) et en cas de confirmation des modifications, la séquence d'étapes suivante :

d) exécution par le terminal d'une action suite à la confirmation par la carte ;

e) en cas de bonne exécution de ladite action par le terminal, inscription dans la carte d'une information de ratification ultérieurement accessible en lecture.

13. Le procédé de la revendication 12, dans lequel la commande d'inscription de l'étape e) est une commande implicite, toute commande reçue par la carte après l'étape b) étant interprétée comme un ordre d'inscription dans la carte d'une information de ratification.

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 89 02140 A (MARS) 9 March 1989 (1989-03-09) cited in the application	1,2,12
A	abstract; claims; figures page 13, line 11 - page 20, line 6	5,6,8,9
Y	US 4 877 945 A (K. FUJISAKI) 31 October 1989 (1989-10-31) cited in the application the whole document	1,2,12
A	DE 44 39 266 A (SIEMENS) 11 April 1996 (1996-04-11) abstract; claims; figure	1-3,5,6, 8,10,12
A	FR 2 701 578 A (GEMPLUS CARD INTERNATIONAL) 19 August 1994 (1994-08-19)	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 August 1999	27/08/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

In ational Application No
PCT/FR 99/00837

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
P,A	FR 2 757 661 A (GEMPLUS) 26 June 1998 (1998-06-26) abstract; claims; figures	1,2,5-7, 12
A	FR 2 689 662 A (GEMPLUS CARD INTERNATIONAL) 8 October 1993 (1993-10-08)	
A	EP 0 740 268 A (FRANCE TELECOM) 30 October 1996 (1996-10-30)	
A	EP 0 700 023 A (KONINKLIJKE PTT NEDERLAND) 6 March 1996 (1996-03-06)	

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 8902140 A	09-03-1989	EP 0389484 A	03-10-1990
		JP 3501302 T	22-03-1991
US 4877945 A	31-10-1989	JP 63120391 A	24-05-1988
DE 4439266 A	11-04-1996	AT 163786 T	15-03-1998
		WO 9610810 A	11-04-1996
		DE 59501580 D	09-04-1998
		EP 0783741 A	16-07-1997
		ES 2113754 T	01-05-1998
		JP 9512368 T	09-12-1997
		US 5889266 A	30-03-1999
FR 2701578 A	19-08-1994	NONE	
FR 2757661 A	26-06-1998	WO 9828719 A	02-07-1998
FR 2689662 A	08-10-1993	NONE	
EP 0740268 A	30-10-1996	FR 2733615 A	31-10-1996
		JP 8305812 A	22-11-1996
		US 5767504 A	16-06-1998
		US 5847374 A	08-12-1998
EP 0700023 A	06-03-1996	NL 9401406 A	01-04-1996
		US 5635695 A	03-06-1997

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 89 02140 A (MARS) 9 mars 1989 (1989-03-09) cité dans la demande	1,2,12
A	abrégé; revendications; figures page 13, ligne 11 - page 20, ligne 6	5,6,8,9
Y	US 4 877 945 A (K. FUJISAKI) 31 octobre 1989 (1989-10-31) cité dans la demande le document en entier	1,2,12
A	DE 44 39 266 A (SIEMENS) 11 avril 1996 (1996-04-11) abrégé; revendications; figure	1-3,5,6, 8,10,12
A	FR 2 701 578 A (GEMPLUS CARD INTERNATIONAL) 19 août 1994 (1994-08-19)	

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
19 août 1999	27/08/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk. Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 99/00837

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
P,A	FR 2 757 661 A (GEMPLUS) 26 juin 1998 (1998-06-26) abrégé; revendications; figures	1,2,5-7, 12
A	FR 2 689 662 A (GEMPLUS CARD INTERNATIONAL) 8 octobre 1993 (1993-10-08)	
A	EP 0 740 268 A (FRANCE TELECOM) 30 octobre 1996 (1996-10-30)	
A	EP 0 700 023 A (KONINKLIJKE PTT NEDERLAND) 6 mars 1996 (1996-03-06)	

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 8902140 A	09-03-1989	EP 0389484 A	03-10-1990
		JP 3501302 T	22-03-1991
US 4877945 A	31-10-1989	JP 63120391 A	24-05-1988
DE 4439266 A	11-04-1996	AT 163786 T	15-03-1998
		WO 9610810 A	11-04-1996
		DE 59501580 D	09-04-1998
		EP 0783741 A	16-07-1997
		ES 2113754 T	01-05-1998
		JP 9512368 T	09-12-1997
		US 5889266 A	30-03-1999
FR 2701578 A	19-08-1994	AUCUN	
FR 2757661 A	26-06-1998	WO 9828719 A	02-07-1998
FR 2689662 A	08-10-1993	AUCUN	
EP 0740268 A	30-10-1996	FR 2733615 A	31-10-1996
		JP 8305812 A	22-11-1996
		US 5767504 A	16-06-1998
		US 5847374 A	08-12-1998
EP 0700023 A	06-03-1996	NL 9401406 A	01-04-1996
		US 5635695 A	03-06-1997

TRAITE D.. COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 29 novembre 1999 (29.11.99)	
Demande internationale no PCT/FR99/00837	**Référence du dossier du déposant ou du mandataire** 464-I51177WO
Date du dépôt international (jour/mois/année) 09 avril 1999 (09.04.99)	**Date de priorité** (jour/mois/année) 09 avril 1998 (09.04.98)
Déposant DIDIER, Stéphane etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

04 novembre 1999 (04.11.99)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Kiwa Mpay

no de téléphone: (41-22) 338.83.38